PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-316963
(43)Date of publication of application : 29.11.1996

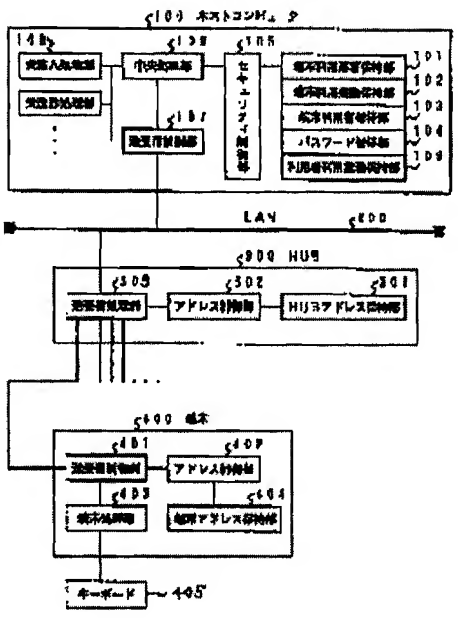
(51)Int.Cl. H04L 12/28
G06F 15/00
H04L 9/32
H04L 12/24
H04L 12/26

(21)Application number : 07-115422
(22)Date of filing : 15.05.1995

(71)Applicant : NEC CORP
(72)Inventor : HARIKAWA KIKUNOSUKE

(54) TERMINAL SECURITY MANAGEMENT DEVICE

(57)Abstract:



PURPOSE: To prevent the wrong use by providing a host computer provided with a user's use application holding part, an application processing part, a central processing part, a security control part, and a transmission/reception control part and a HUB provided with a transmission/reception processing part.

CONSTITUTION: When receiving a start message from a central processing part 106, a security control part 105 checks a user ID and a password holding part 104 to confirm whether the user has the right to the use or not and to identify the user. Next, the control part 105 compares a use application number and a user's use application holding part 109 to confirm whether the user has the right of the use of the application or not and retrieves a terminal user holding part 103 by a terminal address and the user ID to confirm whether the user has the right of the use of the terminal or not. Next, the control part 105 retrieves a terminal's use application holding part 102 by the terminal address and the use application number to confirm whether the terminal has the right of the use or not and retrieves a terminal use place holding part 101 by the terminal address and a HUB address to confirm whether the terminal is used under a correct HUB or not.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平8－316963

(43)公開日　平成８年(1996)11月29日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/28			Ｈ０４Ｌ	11/00	３１０Ｚ
Ｇ０６Ｆ	15/00	３１０	9364－5L	Ｇ０６Ｆ	15/00	３１０Ａ
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	Ａ
	12/24		9466－5K		11/08	
	12/26					

審査請求　有　　請求項の数２　ＯＬ　（全６頁）

(21)出願番号　　特願平7－115422

(22)出願日　　平成７年(1995)５月15日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　針川　菊之介
東京都港区芝五丁目７番１号　日本電気株式会社内

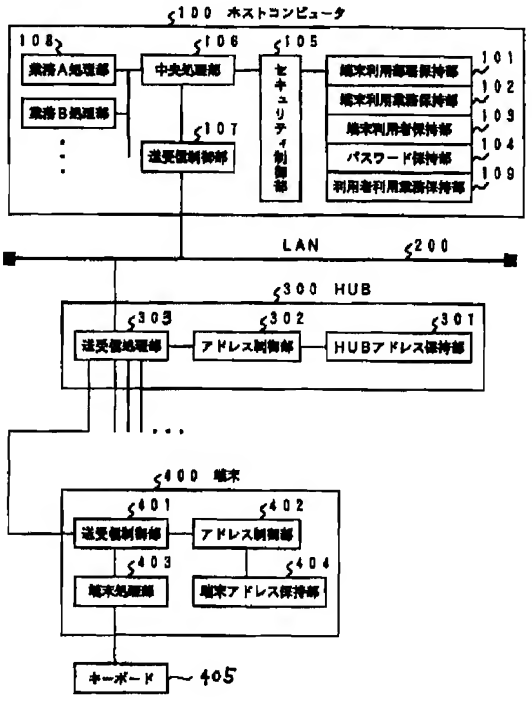
(74)代理人　弁理士　後藤　洋介　（外２名）

(54)【発明の名称】　端末セキュリティ管理装置

(57)【要約】　（修正有）

【目的】　セキュリティ管理上パスワードにより利用者を確認できてもその利用者が悪意を持った場合にも不正利用を防止する。

【構成】　パスワード保持部１０４、セキュリティ制御部１０５、送受信制御部１０７を有するホストコンピュータ１００と、端末４００をＬＡＮ２００に接続するための装置であり、ＬＡＮ上のＨＵＢを一意にするためのアドレスが格納されるＨＵＢアドレス保持部３０１とアドレス制御部３０２と送受信処理部３０３を有するＨＵＢ３００と、自分のアドレスを管理している端末アドレス保持部４０４とアドレス制御部４０２と送受信制御部４０１と端末処理部４０３と利用者のパスワード、処理業務、等を入力するキーボード４０５を有する端末４００から成る。悪意の利用者が利用できる端末が限定され、その端末での業務も限定され、作業場所を限定される。



1

【特許請求の範囲】

【請求項１】　端末毎にその端末が接続できるＨＵＢのアドレスを管理している端末利用部署保持部と端末毎にその端末で処理出来る業務を管理している端末利用業務保持部と端末毎にその端末を利用できる人を管理している端末利用者保持部と利用者ＩＤとその端末利用者が入力するパスワードを管理しているパスワード保持部と利用者が利用できる業務を管理している利用者利用業務保持部及び業務処理部、中央処理部、セキュリティ制御部、送受信制御部とを有するホストコンピュータと、端末をＬＡＮに接続するための装置でありＬＡＮ上のＨＵＢを一意にするためのアドレスが格納されているＨＵＢアドレス保持部とそのアドレスを制御するアドレス制御部とデータの受け渡しを行う送受信処理部とを有するＨＵＢと、自分のアドレスを管理している端末アドレス保持部とそのアドレスを処理するアドレス制御部とメッセージの送受信を行う送受信制御部と端末処理部と利用者のパスワード・処理業務等を入力する入力手段とを有する端末とから成ることを特徴とする端末セキュリティ管理装置。

【請求項２】　請求項１記載の端末セキュリティ管理装置において、前記入力手段はキーボードにより構成されることを特徴とする端末セキュリティ管理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は端末セキュリティ管理装置に関し、特にＬＡＮによるオンライン処理のセキュリティ管理装置に関する。

【０００２】

【従来の技術】従来の端末セキュリティ管理装置は、図２に示すように、アクセス用の端末１及び第一のモデム２を持つアクセス用端末局側から第二のモデム４及び被アクセス用のデータベース５を持つセンター局側へのアクセス時に端末１から入力されたユーザ識別信号をセンター局側で受けて該ユーザのアクセス権の有無を照合し、アクセス権有りの場合に該アクセスを許可する方式において、前記第一のモデム２は、前記アクセス前に予め前記センター局側から発したモデム識別用の第二の識別信号を記憶し、前記アクセス時に前記センター局側から発した送信要求に応答して予め記載されているモデム識別用の第二の識別信号と予め別手段で与えられかつ前記端末１から入力される第二の識別信号とを照合し一致する場合、第二の識別信号を発生し返送するための識別信号を有し前記第二のモデム４は、前記アクセス時に前記送信要求を発した後返送されてくる前記第二の識別信号を受けて前記第一のモデム２のアクセス権の有無を照合するためのモデム識別信号照合手段を有し、前記第一及び第二の識別信号の両照合結果が共にアクセス権有りの場合にのみ該アクセスを許可するようになっている（特開昭６４－４１３８号参照）。尚、図２において、

2

第一のモデム２は、端末インタフェース２０と、送信回路２１と、受信回路２２と、ラインインタフェース２３と、ＩＤ照合・発生回路２４とを有する。また、第二のモデム４は、端末インタフェース４０と、送信回路４１と、受信回路４２と、ラインインタフェース４３と、ＩＤ照合・発生回路４４とを有する。

【０００３】次に、図２に示した従来の端末セキュリティ管理装置の動作について説明する。ＩＤ照合・発生回路２４は、センター局から予めアクセス前に発信するモデム場所を識別するＩＤを記憶するＩＤメモリーを内蔵している。これは予めデータベース５に登録されている電話番号（即ち場所）から正しくアクセスがなされる事を保証するため、予めセンター局から各端末へダイヤルし、個々のモデムＩＤを送信する。各端末側のモデムは、前記ＩＤ照合・発生回路２４のメモリー内に本モデムＩＤを記憶する。またセンター局から端末へ送信されるモデムＩＤと別に、同じモデムＩＤを別のルート（例えばメール等）で端末側へ知らされる。端末局からセンター局へのアクセス時には、端末局から発呼（ダイヤル）を行い、これに対するセンター局の自動応答により公衆電話網３での回線接続が完了する。この後センター局側の第二のモデム４が端末局に対してＩＤ照合・発生回路４４によりモデムＩＤの送信要求を出す。この送信要求を受信した第一のモデム２は端末１に対してモデムＩＤ送信要求を出す。端末１は予め与えられたモデムＩＤ（モデム２にロードされたＩＤとは別ルートでユーザに与えられている）を第一のモデム２へ入力する。第一のモデム２では予めメモリーされているモデムＩＤと比較／照合した後、合致していればモデムＩＤの送信を行う。これを受けたデータベース５は、アクセス権をもつ端末局のモデムＩＤであるか否かを逐一照合し、照合結果がアクセス権有りを示した時だけ肯定応答ＡＣＫを端末局へ送信する。

【０００４】

【発明が解決しようとする課題】この従来のこの方式ではアクセス権確認のためには、端末からモデムＩＤを複数の人が使用する場合全員が同一のモデムＩＤを入力することになり、人毎のアクセス権の確認ができない。

又、ＬＡＮの様に一つの通信回線で一カ所に複数の端末を設置する場合、端末毎にモデムを設置しなければならずＨＵＢの様な機器（一つの機器で複数の端末をＬＡＮに接続する機器）の場合は対応できないという問題がある。

【０００５】

【課題を解決するための手段】本発明によれば、端末毎にその端末が接続できるＨＵＢのアドレスを管理している端末利用部署保持部と端末毎にその端末で処理出来る業務を管理している端末利用業務保持部と端末毎にその端末を利用できる人を管理している端末利用者保持部と利用者ＩＤとその端末利用者が入力するパスワードを管

理しているパスワード保持部と利用者が利用できる業務を管理している利用者利用業務保持部及び業務処理部、中央処理部、セキュリティ制御部、送受信制御部とを有するホストコンピュータと、端末をＬＡＮに接続するための装置でありＬＡＮ上のＨＵＢを一意にするためのアドレスが格納されているＨＵＢアドレス保持部とそのアドレスを制御するアドレス制御部とデータの受け渡しを行う送受信処理部とを有するＨＵＢと、自分のアドレスを管理している端末アドレス保持部とそのアドレスを処理するアドレス制御部とメッセージの送受信を行う送受信制御部と端末処理部と利用者のパスワード・処理業務等を入力する入力手段とを有する端末とから成ることを特徴とする端末セキュリティ管理装置が得られる。

【０００６】また、本発明によれば、前記入力手段はキーボードにより構成されることを特徴とする端末セキュリティ管理装置が得られる。

【０００７】

【実施例】次に、本発明の実施例に係る端末セキュリティ管理装置について図面を参照して説明する。

【０００８】本実施例の端末セキュリティ管理装置は、図１に示すように、端末毎にその端末が接続できるＨＵＢ３００のアドレスを管理している端末利用部署保持部１０１と端末毎にその端末で処理出来る業務を管理している端末利用業務保持部１０２と端末毎にその端末を利用できる人を管理している端末利用者保持部１０３と利用者ＩＤとその端末利用者が入力するパスワードを管理しているパスワード保持部１０４と利用者が利用できる業務を管理している利用者利用業務保持部１０９及び業務Ａ処理部１０８等の業務処理部、中央処理部１０６、セキュリティ制御部１０５、送受信制御部１０７を有するホストコンピュータ１００と、端末４００をＬＡＮ２００に接続するための装置であるが、ＬＡＮ上のＨＵＢを一意にするためのアドレスが格納されているＨＵＢアドレス保持部３０１とそのアドレスを制御するアドレス制御部３０２とデータの受け渡しを行う送受信処理部３０３を有するＨＵＢ３００と、自分のアドレスを管理している端末アドレス保持部４０４とそのアドレスを処理するアドレス制御部４０２とメッセージの送受信を行う送受信制御部４０１と端末処理部４０３と利用者のパスワード、処理業務、等を入力するキーボード４０５を有する端末４００から成る。

【０００９】即ち、ホストコンピュータ１００は端末利用部署保持部１０１と端末利用業務保持部１０２と端末利用者保持部１０３とパスワード保持部１０４と業務Ａ処理部１０８等の業務処理部と中央処理部１０６とセキュリティ制御部１０５と送受信制御部１０７と利用者利用業務保持部１０９から成る。端末利用部署保持部１０１は端末毎に（端末アドレス毎に）その端末が接続できるＨＵＢ３００のアドレスを管理しておりつまり、これによりその端末が使える部署が限定できる。端末利用業務保持部１０２は端末毎に（端末アドレス毎に）その端末で処理出来る業務名を管理しており、これによりその端末で利用できる業務（処理範囲）を限定できる。端末利用者保持部１０３は端末毎に（端末アドレス毎に）その端末を利用できる人（利用者のＩＤ番号で個人を認識し、その個人のＩＤ番号は端末より入力される）を管理しており、これにより個人毎に利用できる端末を限定できる。パスワード保持部１０４は利用者毎に利用者ＩＤと利用者の暗唱番号を管理しており、他人による個人ＩＤの不正使用を防止する。利用者利用業務保持部１０９は利用者毎にその利用者が利用出来る業務を管理しており利用者が利用出来る業務を制限できる。セキュリティ制御部１０５はホストコンピュータで受け取ったセキュリティ情報をもとに端末利用部署保持部１０１、端末利用業務保持部１０２、端末利用者保持部１０３、パスワード保持部１０４及び利用者利用業務保持部１０９の情報を確認し利用権の妥当性確認を行う。

【００１０】中央処理部１０６はホストコンピュータの全体処理を行う。送受信制御部１０７はＬＡＮとのデータ通信を行う。業務Ａ処理部１０８等の業務処理部は、複数の各業務処理部から成り各端末との実際の業務処理を行う。

【００１１】ＬＡＮ２００はデータ通信を行うための通信回線でありＬＡＮ上には一つのホストコンピュータと複数の端末接続用ＨＡＢが接続される。

【００１２】ＨＵＢ３００はＬＡＮに端末を接続するための装置で有り一つのＨＵＢには複数の端末を接続することができる。また、ＨＵＢはＨＵＢアドレス保持部３０１、アドレス制御部３０２及び送受信処理部３０３から成る。ＨＵＢアドレス保持部３０１は全体でＨＵＢを一意に識別するためのアドレス（番号）が格納されており端末のオンライン開始時このアドレスがホストコンピュータに通知される、ホストコンピュータではこれにより端末がどこの部署（ＨＵＢ配下）で使用されようとしているか知ることができる。アドレス制御部３０２は端末のオンライン開始時ＨＵＢアドレス保持部よりＨＵＢのアドレスを入手しホストコンピュータへ通知する。送受信処理部３０３はＬＡＮと端末とのデータ通信を行うが端末がオンライン開始する場合はアドレス制御部３０２へＨＵＢのアドレス取得を指示しその結果をホストコンピュータへ通知する役割もある。

【００１３】端末４００はホストコンピュータと業務処理用端末で、送受信制御部４０１、アドレス制御部４０２、端末処理部４０３、端末アドレス保持部４０４及びキーボード４０５からなる。送受信制御部４０１はＨＵＢとのデータ通信を行う装置であるがＨＵＢに対してデータを送信する場合はアドレス制御部４０２に対して端末アドレスの取得を指示し、その結果の端末アドレスをメッセージに付加し送信する。アドレス制御部４０２は送受信制御部４０１の指示に従い、端末アドレス保持部

４０４より端末アドレスを取得し送受信制御部４０１へ通知する。端末アドレス保持部４０４は全端末を一意に識別するためのアドレス（番号）が格納されており、このアドレスをホストコンピュータとの送受信メッセージに付加することによりホストコンピュータは端末を一意に識別できる。キーボード４０５は端末側でオンライン開始時は利用者ＩＤ、パスワード及びオンラインの利用業務を入力する。

【００１４】次に動作について説明する。端末よりオンライン処理を行う場合まず端末４００のキーボード４０５より利用者のＩＤ、パスワード及び利用したい業務を入力する。入力されたデータは端末処理部４０３でオンライン開始の送信メッセージとして送受信制御部４０１へ渡される。送受信制御部４０１はアドレス制御部４０２へ指示し端末アドレス保持部４０４より端末アドレスを入手し送信メッセージに端末アドレスを付加しＨＵＢ３００へ渡す。

【００１５】ＨＵＢ３００は送受信処理部３０３で端末４００からのメッセージを受け取りオンライン開始メッセージかどうかの判断を行いオンライン開始メッセージであればアドレス制御部３０２へ指示しＨＵＢアドレス保持部３０１よりＨＡＢアドレスを入手しオンライン開始メッセージのＨＵＢアドレスを付加しＬＡＮ２００へメッセージを送信する。

【００１６】オンライン開始メッセージはＬＡＮ２００を通りホストコンピュータ１００へ通知される。

【００１７】ホストコンピュータ１００ではＬＡＮ２００からのメッセージを送受信制御部１０７で受け取り中央処理部１０６へ渡す。中央処理部１０６はオンライン開始メッセージの場合そのメッセージをセキュリティ制御部１０５へ渡しオンライン利用権の合否判定を行う。合否判定の結果合格であれば業務Ａ処理部１０８等の業務処理部に対してメッセージを渡し、以降端末４００との業務処理がおこなわれる。不合格であれば、利用権なしのメッセージを送受信制御部１０７を介して端末４００へ通知する。セキュリティ制御部１０５は中央処理部１０６よりオンライン開始メッセージを受け取ると、まずメッセージ中の利用者ＩＤとパスワードによりパスワード保持部１０４を調べ利用者のオンライン利用権が有るか又、パスワードにより利用者本人かどうか確認する。次にメッセージ中の利用業務番号と利用者利用業務保持部１０９とを比較しその利用者が指定した業務が利用できる権利があるか確認する。次にメッセージ中の端末アドレスと利用者ＩＤにより端末利用者保持部１０３を検索しその利用者がその端末の利用権が有るかどうかを確認する。次に、メッセージ中の端末アドレスと利用業務番号により端末利用業務保持部１０２を検索しその端末で指定の業務の利用権があるか確認する。次にメッセージ中の端末アドレスとＨＵＢアドレスにより端末利用部署保持部１０１を検索しその端末が正しいＨＵＢ配下（正しい部署）で使用されているか確認する。これらの確認がすべて正しい（ＯＫ）の場合にセキュリティ制御部１０５は中央処理部１０６に対して合格を通知し一つでも不正があれば不合格を通知する。

【００１８】

【発明の効果】以上説明したように、本発明は、悪意を持った利用者であっても利用できる端末が限定され、その端末で利用できる業務も限定され、さらに作業できる場所が限定され、またその場所に管理者が居ることを考えれば基本的には不正利用を防止できるという効果を有する。

【図面の簡単な説明】

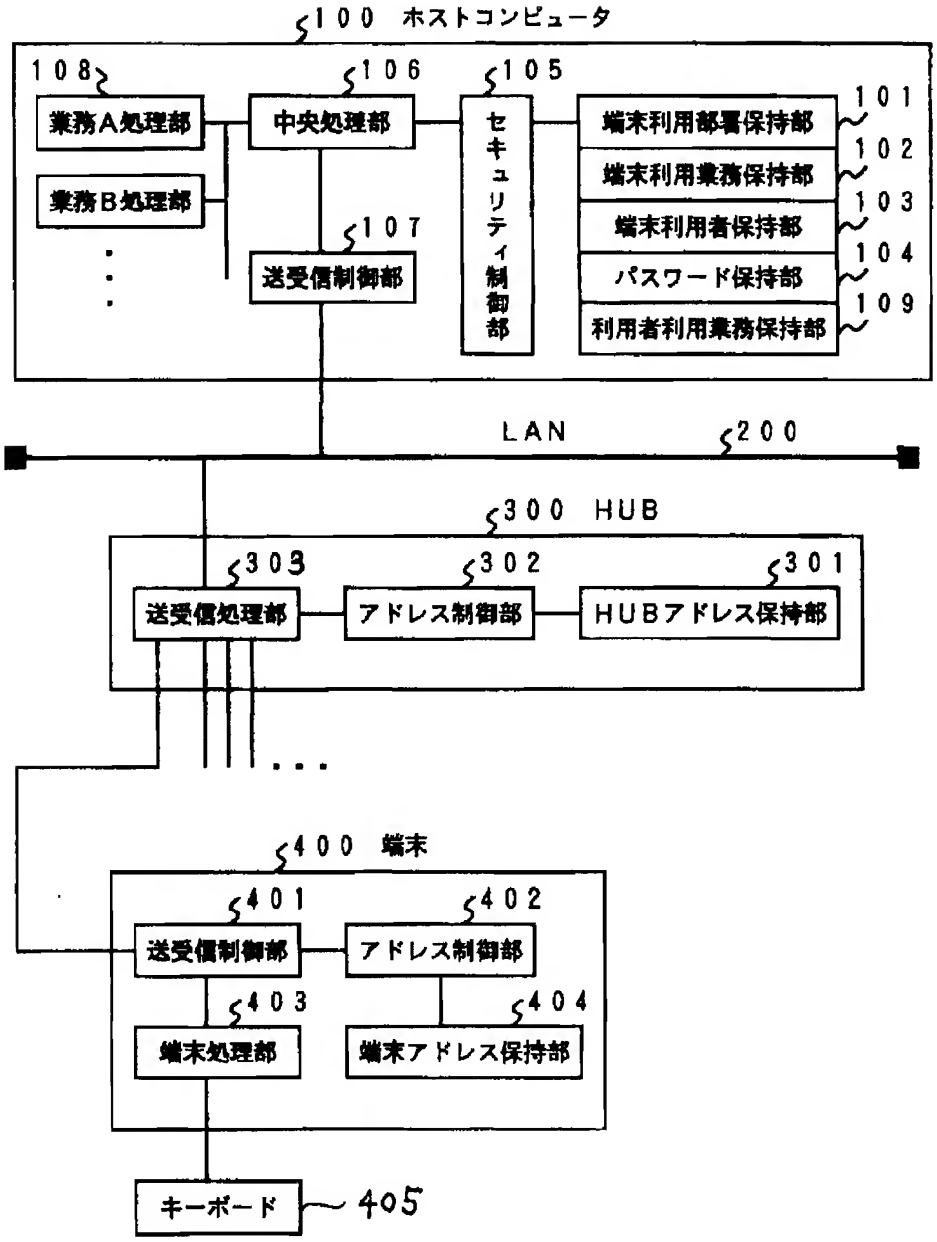
【図１】本発明の実施例に係る端末セキュリティ管理装置のブロック図である。

【図２】従来の端末セキュリティ管理装置のブロック図である。

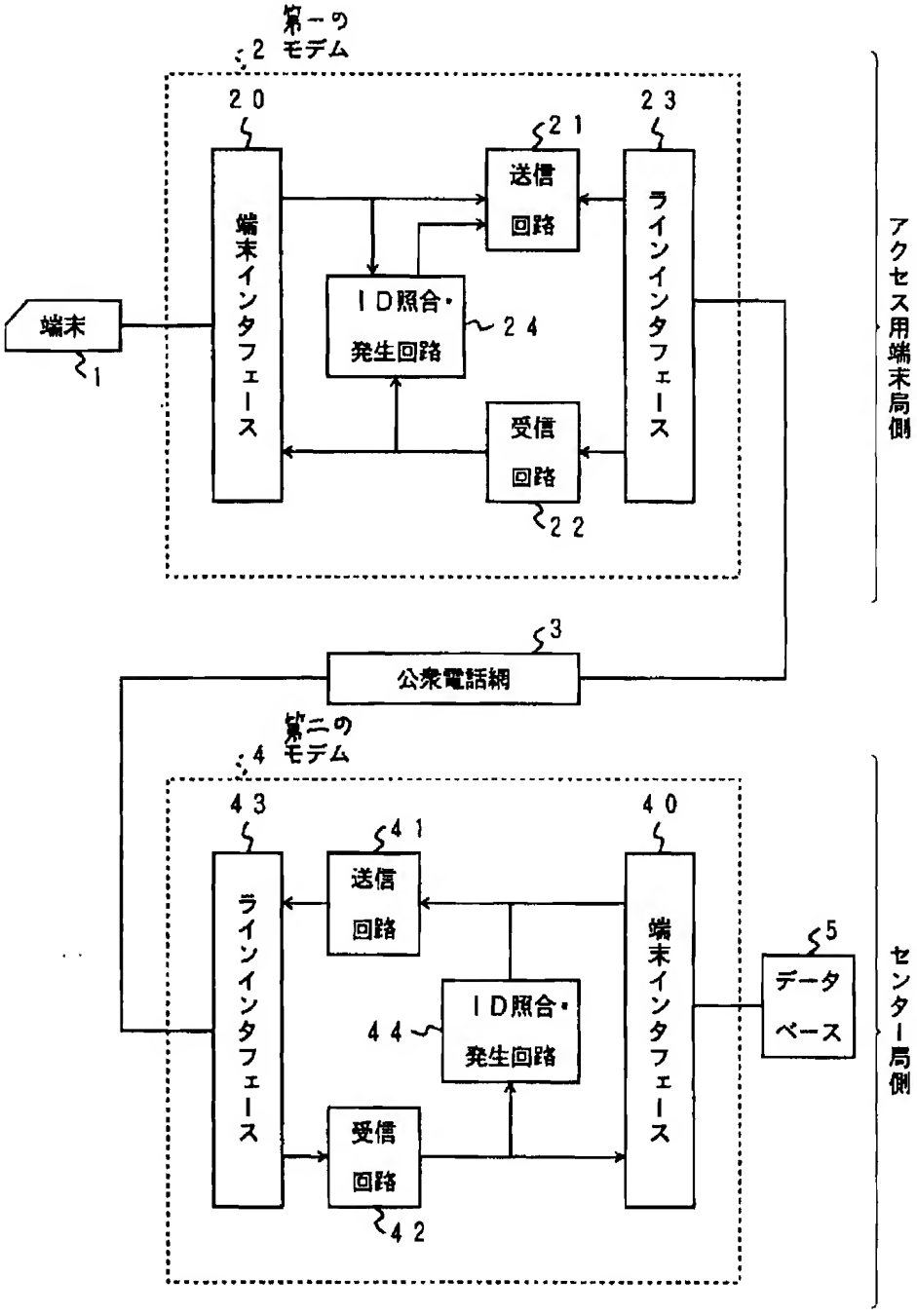
【符号に説明】

１００	ホストコンピュータ
１０１	端末利用部署保持部
１０２	端末利用業務保持部
１０３	端末利用者保持部
１０４	パスワード保持部
１０５	セキュリティ制御部
１０６	中央処理部
１０７	送受信制御部
１０８	業務Ａ処理部
１０９	利用者利用業務保持部
２００	ＬＡＮ
３００	ＨＵＢ
３０１	ＨＵＢアドレス保持部
３０２	アドレス制御部
３０３	送受信処理部
４００	端末
４０１	送受信制御部
４０２	アドレス制御部
４０３	端末処理部
４０４	端末アドレス保持部
４０５	キーボード

【図1】


100 ホストコンピュータ
108
業務A処理部
業務B処理部
106
中央処理部
107
送受信制御部
105
セキュリティ制御部
端末利用部署保持部
端末利用業務保持部
端末利用者保持部
パスワード保持部
利用者利用業務保持部
101
102
103
104
109
LAN
200
300 HUB
303
送受信処理部
302
アドレス制御部
301
HUBアドレス保持部
400 端末
401
送受信制御部
402
アドレス制御部
403
端末処理部
404
端末アドレス保持部
キーボード
405

【図2】


第一の
2 モデム
20
21
23
端末インタフェース
送信回路
ラインインタフェース
端末
1
ID照合・発生回路
24
受信回路
22
アクセス用端末局側
3
公衆電話網
第二の
4 モデム
43
41
40
ラインインタフェース
送信回路
端末インタフェース
5
データベース
44
ID照合・発生回路
受信回路
42
センター局側